C&A Point Paper

The intent of this paper is to describe the federal and Departmental requirements for certification and accreditation, explain the Department's current certification and accreditation strategy, and provide alternative approaches.

The key cost drivers for C&A are preparing the C&A package, executing the test plans, and mitigating discovered risks.

Federal Requirements overview

OMB Circular A-130 requires that federal organizations ensure that a management official authorizes in writing the use of each general support system and major application. Management authorization should be based on an assessment of management, operational, and technical controls.

- Some agencies perform "certification reviews" of their systems periodically.
- These formal technical evaluations lead to a management accreditation, or "authorization to process."

The Federal Information Security Reform Act (FISMA) requires annual self-assessments, historically performed using NIST 800-26. A critical element within the document requires systems to be certified and authorized to process (accredited). FISMA itself does not require C&A but it does require Agencies to report to OMB quarterly. ED has promised OMB that the Department would C&A its systems by 12/31/02.

Each Department creates its own implementation procedures based on the federal guidance.

- NIST 800-37 currently is in draft. Expected release date is summer 2003
- NIST 800-53, 800-53a (security control implementation documents) are expected to be released in the Fall 2003.
- Until these documents are approved, the Department has flexibility in its C&A strategy.

ED/OCIO's current C&A approach

- The Department's C&A strategy is articulated in a document titled *IT Security Certification and Accreditation Procedures*. The C&A strategy is based on the National Information Assurance Certification and Accreditation Process (NIACAP), which was initially designed for classified, non-DoD information systems.
- Last year, FSA and OCIO agreed to license a C&A tool (roughly $500K) that will assist the Department create a consistent C&A program across its numerous Principle Offices and expedite the process itself. The tool does the following:
    - o Assists systems organize its security information create the System Security Authorization Agreement (SSAA) required by the Department,

  - Generates an ST&E based on a pre-populated federal, Departmental, and FSA security requirements traceability matrix (SRTM).
  - The SRTM contains all relevant security requirements and associated test procedures.
  - The C&A tool lessens the cost, in terms of labor hours, of creating the SSAA and ST&E and eliminates the need for all systems to generate security requirements separately.

- Department's C&A strategy:
  - All tier 3 and 4 systems will be certified and accredited by December 31, 2003;
  - All tier 1 and 2 systems certified and accredited by December 31, 2004.
  - An OCIO sponsored Certification Review Group (CRG) will execute Security Test and Evaluation plans prepared by individual systems.
  - Based on the results of the tests, the CRG will make a certification recommendation to the Certifying Official (ED CIO), who in turn will make an accrediting recommendation to a Designated Approving Authority (DAA).
  - The DAA (business owner) will approve full accreditation, issue an interim authority to operate (IATO), or deny accreditation.
  - Under the current strategy, every tier 3 and 4 system is to create an SSAA, ST&E and provide all security documentation to the CRG by August 4, 2003.
  - According to the Department's C&A guide, tier 4 systems must have penetration tests and vulnerability scans as part of the certification testing. Tier 3 systems are only recommended to have penetration tests and vulnerability scans. The C&A guide does not detail what components of a system require penetration tests or vulnerability scans, so some interpretation is available.
  - Once the CRG completes the tests, all systems will have findings or weaknesses. These weaknesses will need to be remediated. The amount and cost of the remediation effort will remain unknown until the testing and cost/benefit analyses are performed.
  - The unreleased SOW for the CRG identifies completing 21-23 Tier 3&4 system and 6 Tier 1&2 systems by 9/30/03.
  - Several optional tasks are included in the SOW that could be eliminated to save cost.

Alternative Approaches

Eliminate SSAA

The pre-draft NIST Special Publication 800-37 Guide for Security Certification and Accreditation of Federal Information Technology Systems eliminates the requirement for an SSAA, only requiring a system security plan, risk assessment, and an ST&E. The current Department strategy requires the SSAA because of its intent to adhere to NIACAP. NIACAP is not required of civilian, unclassified systems, but is considered a viable option for C&A.

Benefits:

- Eliminate largely redundant document.
- Moves entire Department to anticipated new federal standard

Drawbacks:

- New federal standard is still in pre-draft resulting in some risk for ED.
- Invested in C&A tool partly because of the requirement to create the cumbersome SSAA. Could be viewed as ineffective planning by management.
- Centralized repository of information no longer available.

Cost Implications: Labor hours are eliminated for data entry into C&A tool.

Limit comprehensiveness of CRG tests

A major cost driver of C&A is the testing or validation of security controls. In security, one can always perform more tests. The key is to determine what level of assurance senior management needs to determine whether security controls operate in the way they were intended. Security testing is performed using one of the following techniques: documentation review, interview, observation or technical evaluation (test). Each progressive test performed provides increased assurance for senior management that controls operate as intended. OCIO could limit the amount of technical evaluations conducted on system components, limit/ eliminate on-site evaluations, perform all interviews via telephone, and rely heavily on documentation. These measures significantly reduce the cost of testing, but the assurance level decreases.

Benefits:

- Decrease the costs of C&A testing
- Decrease the time required to execute ST&E

Drawbacks:

- Assurance level decreases leaving management less certain that security controls are implemented adequately
- Independent evaluations by IG/GAO may reject certifications based on inadequate testing

Cost Implications:

- Labor hours necessary to execute ST&E decreases

Status quo

FSA will complete its SSAAs and ST&Es by the August 4th deadline for its Tier 3 and 4 systems. All FSA systems will submit certification packages to the CRG and will support the CRG during the testing period. Other Department systems may have more difficulty reaching this deadline because their systems are not as thoroughly documented.

Benefits:
- Department continues along its C&A plan of action
- System personnel are not forced to alter current plan
- Better position versus audit community

Drawbacks:
- ED may not meet self-imposed deadline to OMB.

Cost Implications:
- To C&A 21 systems, with generally agreed upon certification levels of testing, the cost has been estimated by OCIO at $4.5million. The calculation breaks down to 4 people per system, at $100 an hour for just over 3 months.